IN THE DRAWINGS:

Please replace originally filed Fig. 3 with replacement Fig. 3 attached hereto, wherein the text "SECOND IDENTIFYING INFORMATION" is amended to "SIGNATURE IDENTIFYING INFORMATION" in block 240 (two occasions), the text "SECOND RECEIPT INFORMATION" is amended to "SIGNATURE RECEIPT INFORMATION" in block 250 (one occasion), and the text "THIRD IDENTIFYING INFORMATION" is amended to "SIGNATURE RECEIPT IDENTIFYING INFORMATION" in block 255 (one occasion).

Please replace originally filed Fig. 4 with replacement Fig. 4 attached hereto, wherein the text "THE REPOSITORY REQUESTS A PARTIAL MESSAGE DIGEST" is amended to "THE REMOTE LOCATION REQUESTS A PARTIAL MESSAGE DIGEST" in block S435 (one occasion).

Please replace originally filed Fig. 7 with replacement Fig. 7 attached hereto, wherein the term "ENCRYPTION" is amended to "CRYPTOGRAPHIC" in block S735 (one occasion).

Please replace originally filed Fig. 8 with replacement Fig. 8 attached hereto, wherein the text "SECOND IDENTIFYING INFORMATION" is amended to "SIGNATURE IDENTIFYING INFORMATION" in block S820 (one occasion), the text "SECOND RECEIPT INFORMATION" is amended to "SIGNATURE RECEIPT INFORMATION" in block S825 (one occasion), the text "SECOND RECEIPT INFORMATION" is amended to "SIGNATURE RECEIPT INFORMATION" in block S830 (one occasion), the text "THIRD IDENTIFYING INFORMATION" is amended to "SIGNATURE RECEIPT IDENTIFYING INFORMATION" in block S835 (one occasion), and the text "THIRD IDENTIFYING INFORMATION" is amended to "SIGNATURE RECEIPT IDENTIFYING INFORMATION" in block S340 (one occasion).

REMARKS

Claims 1, 2, 4-8, 11-14, 16-18, 20-24, 28, 30-34, and 36-50 are pending in this application. By this Amendment, claims 1-2, 5-7, 11-14, 16-18, 21-24, 30-34, and 36-40 are amended to further clarify the recited subject matter, original claims 3, 9, 10, 15, 19, 25, 26, 27, 29, and 35 are canceled, and new claims 41-50 are added. Originally filed Figs. 3, 4, 7, and 8 are replaced with new Figs. 3, 4, 7, and 8. The above-indicated amendments are supported by the original disclosure and no new matter is added by these amendments. Reconsideration in view of the following remarks is respectfully requested.

By this Amendment, a substitute specification and abstract have been filed to further clarify the originally disclosed subject matter. Applicant believes that the substitute specification includes no new matter. No subject matter is added by these amendments that was not disclosed in the application as originally filed. Reconsideration in view of the above amendments and the following remarks is respectfully requested.

I. PRIOR ART REJECTIONS - 35 U.S.C. §102

A. CLAIMS 17, 18, 20, 21, AND 37 ARE PATENTABLE OVER BISBEE ET AL.

The Office Action rejected claims 17, 21, and 37 under 35 U.S.C. §102(b) as being unpatentable over Bisbee et al. (U.S. Patent No. 5,748,738, hereinafter "Bisbee"). The Applicant traverses the rejection because Bisbee fails to teach or suggest all of the features recited in the rejected claims.

i. CLAIMS 17, 18, AND 20 ARE PATENTABLE OVER BISBEE

For example, Bisbee fails to teach or suggest a method for creating a unique authoritative electronic record in a repository, comprising "receiving an original electronic record in a repository; generating at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record, and wherein the first receipt information is prevented from being transmitted outside the repository; prepending the first receipt information at a beginning portion of the original electronic record; generating at least some first identifying information, wherein the first identifying information includes a provable representation of the first receipt information; appending the first identifying information at an end portion of the original electronic record; and storing the original electronic record with the prepended first receipt information and the appended first identifying information in the repository as a unique, authoritative electronic record" (emphasis added), as recited in amended claim 17.

In contrast, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee)

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document.

Therefore, Bisbee fails to teach or suggest and, in fact, teaches away from a method for creating a unique authoritative electronic record in a repository, comprising "receiving an

original electronic record in a repository; generating at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record, and wherein the first receipt information is prevented from being transmitted outside the repository; prepending the first receipt information at a beginning portion of the original electronic record; generating at least some first identifying information, wherein the first identifying information includes a provable representation of the first receipt information; appending the first identifying information at an end portion of the original electronic record; and storing the original electronic record with the prepended first receipt information and the appended first identifying information in the repository as a unique, authoritative electronic record" (emphasis added), as recited in amended claim 17.

Accordingly, Applicant respectfully submits that independent claim 17, is patentable over Bisbee. Likewise, currently pending claims 18 and 20, which depend, either directly or indirectly, from independent claim 17, are also patentable over Bisbee for the reasons discussed above plus the additional feature(s) they recite. Thus, claims 17, 18, and 20 are allowable and withdrawal of the rejection of these claims under 35 U.S.C. §102 is respectfully requested.

ii. CLAIM 21 IS PATENTABLE OVER BISBEE

For example, Bisbee fails to teach or suggest a method for storing an original electronic record as a unique, authoritative electronic record in a repository, comprising "transmitting an original electronic record to a repository; allowing at least some first receipt information to be generated, wherein the first receipt information includes information relating to the original electronic record, and wherein the first receipt information is prevented from being transmitted outside the repository; allowing the first receipt information to be prepended at a beginning portion of the original electronic record; allowing at least some first identifying information to be generated, wherein the first identifying information includes a provable representation of the first receipt information; allowing the first identifying information to be appended at an end portion of the original electronic record; and allowing the original electronic record to be stored with the prepended first receipt information and the appended first identifying information in the repository as a unique, authoritative electronic record" (emphasis added), as recited in amended claim 21.

As discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original

execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee)

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document.

Therefore, Bisbee fails to teach or suggest and, in fact, teaches away from a method for storing an original electronic record as a unique, authoritative electronic record in a repository, comprising "transmitting an original electronic record to a repository; allowing at least some first receipt information to be generated, wherein the first receipt information

includes information relating to the original electronic record, and wherein the first receipt information is prevented from being transmitted outside the repository; allowing the first receipt information to be prepended at a beginning portion of the original electronic record; allowing at least some first identifying information to be generated, wherein the first identifying information includes a provable representation of the first receipt information; allowing the first identifying information to be appended at an end portion of the original electronic record; and allowing the original electronic record to be stored with the prepended first receipt information and the appended first identifying information in the repository as a unique, authoritative electronic record" (emphasis added), as recited in amended claim 21.

Accordingly, Applicant respectfully submits that independent claim 21, is patentable over Bisbee. Thus, claim 21 is allowable and withdrawal of the rejection of this claim under 35 U.S.C. §102 is respectfully requested.

iii. CLAIM 37 IS PATENTABLE OVER BISBEE

For example, Bisbee fails to teach or suggest a system for creating a unique, authoritative electronic record in a repository, comprising "a software program that is capable of receiving an original electronic record in a repository; a software program that is capable of generating at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record, and wherein the first receipt information is prevented from being transmitted outside the repository; a software program that is capable of prepending the first receipt information at a beginning portion of the original electronic record; a software program that is capable of generating at least some first identifying information, wherein the first identifying information includes a provable representation of the first receipt information; a software program that is capable of appending the first identifying information at an end portion of the original electronic record; a software program that is capable of storing the original electronic record with the prepended first receipt information and the appended first identifying information in the repository as a unique, authoritative electronic record" (emphasis added), as recited in amended claim 37.

In contrast, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee)

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document.

Therefore, Bisbee fails to teach or suggest and, in fact, teaches away from a system for creating a unique, authoritative electronic record in a repository, comprising "a software program that is capable of receiving an original electronic record in a repository; a software program that is capable of generating at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record, and wherein the first receipt information is prevented from being transmitted outside the

repository; a software program that is capable of prepending the first receipt information at a beginning portion of the original electronic record; a software program that is capable of generating at least some first identifying information, wherein the first identifying information includes a provable representation of the first receipt information; a software program that is capable of appending the first identifying information at an end portion of the original electronic record; a software program that is capable of storing the original electronic record with the prepended first receipt information and the appended first identifying information in the repository as a unique, authoritative electronic record" (emphasis added), as recited in amended claim 37.

Accordingly, Applicant respectfully submits that independent claim 37, is patentable over Bisbee. Thus, claim 37 is allowable and withdrawal of the rejection of this claim under 35 U.S.C. §102 is respectfully requested.

II. PRIOR ART REJECTIONS - 35 U.S.C. §103

A. CLAIMS 1-2, 4-8, 11-14, 16, 22-24, 28, 30-34, 36, AND 38-40 ARE PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

The Office Action rejected claims 1-16, 18-20, 22-36, and 38-40 under 35 U.S.C. §103(a) as being unpatentable over Bisbee et al. (U.S. Patent No. 5,748,738, hereinafter "Bisbee") in view of Vanstone (U.S. Patent No. 6,212,281, hereinafter "Vanstone"). The Applicant traverses the rejection because the combined teachings of Bisbee and Vanstone fail to teach all of the features recited in the rejected claims.

i. CLAIMS 1-2, 4-8, AND 11-14 ARE PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest a method for obtaining a method in a computer system for maintaining and digitally signing a unique, authoritative electronic record, comprising "receiving an original electronic record in a repository; generating at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record, and wherein the first receipt information is prevented from being transmitted outside the repository; prepending the first receipt information at a beginning portion of the original electronic record; generating at least some first identifying information, wherein the first identifying information includes a provable representation of the first receipt information; appending the first identifying information at an end portion of the original electronic record; storing the original electronic record with the

prepended first receipt information and the appended first identifying information in the repository as a unique, authoritative electronic record; receiving a request to review and optionally sign the authoritative electronic record at a remote location; computing a partially completed message digest of the authoritative electronic record, wherein the partially completed message digest is related to a proper subset of the authoritative electronic record; computing a complement of the proper subset of the authoritative electronic record; transmitting to the remote location the partially completed message digest of the authoritative electronic record; transmitting to the remote location the complement of the proper subset of the authoritative electronic record; completing the computation of the message digest of the authoritative electronic record, at the remote location, using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; displaying the complement of the proper subset of the authoritative electronic record at the remote location; allowing the generation of at least some digital signature information at the remote location, wherein the digital signature information is generated using a private key and the message digest of the authoritative electronic record; returning the digital signature information to the repository; receiving the digital signature information in the repository; determining whether the digital signature information represents a valid digital signature; amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information; generating at least some additional receipt information, wherein the additional receipt information includes information relating to the signed authoritative electronic record; prepending the additional receipt information at a beginning portion of the signed authoritative electronic record; generating at least some additional identifying information, wherein the additional identifying information includes a provable representation of the additional receipt information; appending the additional identifying information at an end portion of the signed authoritative electronic record; and storing the signed authoritative electronic record, the additional receipt information, and the additional identifying information, in the repository as the authoritative electronic record, wherein the signed authoritative electronic record includes the digital signature information" (emphasis added), as recited in amended claim 1.

In contrast, as discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the

original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing

the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document. Additionally, Bisbee discloses forwarding the actual electronic document for review and execution and then, upon receipt of the executed electronic document, authenticating the received electronic document with the appended electronic signature.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest "computing a partial message digest of a proper subset of the authoritative electronic record; transmitting the partial message digest of the authoritative electronic record to the remote location and computing a message digest, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record", as recited in original claim 1.

Applicant submits that, among other features, Bisbee fails to teach or suggest "computing a partially completed message digest of the authoritative electronic record, wherein the partially completed message digest is related to a proper subset of the authoritative electronic record; computing a complement of the proper subset of the authoritative electronic record; transmitting to the remote location the partially completed message digest of the authoritative electronic record; transmitting to the remote location the complement of the proper subset of the authoritative electronic record; completing the computation of the message digest of the authoritative electronic record, at the remote location, using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record", as recited in amended claim 1. Thus, Bisbee fails to teach the claimed subject matter of amended claim 1.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair

that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a method for obtaining a method in a computer system for maintaining and digitally signing a unique, authoritative electronic record, comprising "receiving an original electronic record in a repository; generating at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record, and wherein the first receipt information is prevented from being transmitted outside the repository; prepending the first receipt information at a beginning portion of the original electronic record; generating at least some first identifying information, wherein the first identifying information includes a provable representation of the first receipt information; appending the first identifying information at an end portion of the original electronic record; storing the original electronic record with the prepended first receipt information and the appended first identifying information in the repository as a unique, authoritative electronic record; receiving a request to review and optionally sign the authoritative electronic record at a remote location; computing a partially completed message digest of the authoritative electronic record, wherein the partially completed message digest is related to a proper subset of the authoritative electronic record; computing a complement of the proper subset of the authoritative electronic record; transmitting to the remote location the partially completed message digest of the authoritative electronic record; transmitting to the remote location the complement of the proper subset of the authoritative electronic record; completing the computation of the message digest of the authoritative electronic record, at the remote location, using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; displaying the complement of the proper subset of the

authoritative electronic record at the remote location; allowing the generation of at least some digital signature information at the remote location, wherein the digital signature information is generated using a private key and the message digest of the authoritative electronic record; returning the digital signature information to the repository; receiving the digital signature information in the repository; determining whether the digital signature information represents a valid digital signature; amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information; generating at least some additional receipt information, wherein the additional receipt information includes information relating to the signed authoritative electronic record; prepending the additional receipt information at a beginning portion of the signed authoritative electronic record; generating at least some additional identifying information, wherein the additional identifying information includes a provable representation of the additional receipt information; appending the additional identifying information at an end portion of the signed authoritative electronic record; and storing the signed authoritative electronic record, the additional receipt information, and the additional identifying information, in the repository as the authoritative electronic record, wherein the signed authoritative electronic record includes the digital signature information" (emphasis added), as recited in amended claim 1, and fail to overcome the deficiencies of Bisbee.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a method for obtaining a method in a computer system for maintaining and digitally signing a unique, authoritative electronic record, comprising "receiving an original electronic record in a repository; generating at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record, and wherein the first receipt information is prevented from being transmitted outside the repository; prepending the first receipt information at a beginning portion of the original electronic record; generating at least some first identifying information, wherein the first identifying information includes a provable representation of the first receipt information; appending the first identifying information at an end portion of the original electronic record; storing the original electronic record with the prepended first receipt information and the appended first identifying information in the repository as a

unique, authoritative electronic record; receiving a request to review and optionally sign the authoritative electronic record at a remote location; computing a partially completed message digest of the authoritative electronic record, wherein the partially completed message digest is related to a proper subset of the authoritative electronic record; computing a complement of the proper subset of the authoritative electronic record; transmitting to the remote location the partially completed message digest of the authoritative electronic record; transmitting to the remote location the complement of the proper subset of the authoritative electronic record; completing the computation of the message digest of the authoritative electronic record, at the remote location, using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; displaying the complement of the proper subset of the authoritative electronic record at the remote location; allowing the generation of at least some digital signature information at the remote location, wherein the digital signature information is generated using a private key and the message digest of the authoritative electronic record; returning the digital signature information to the repository; receiving the digital signature information in the repository; determining whether the digital signature information represents a valid digital signature; amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information; generating at least some additional receipt information, wherein the additional receipt information includes information relating to the signed authoritative electronic record; prepending the additional receipt information at a beginning portion of the signed authoritative electronic record; generating at least some additional identifying information, wherein the additional identifying information includes a provable representation of the additional receipt information; appending the additional identifying information at an end portion of the signed authoritative electronic record; and storing the signed authoritative electronic record, the additional receipt information, and the additional identifying information, in the repository as the authoritative electronic record, wherein the signed authoritative electronic record includes the digital signature information" (emphasis added), as recited in amended claim 1.

Therefore, Applicant respectfully submits that independent claim 1 is patentable over Bisbee in view of Vanstone. Likewise, dependent claims 2, 4-8, and 11-14 are also patentable over Bisbee in view of Vanstone by virtue of their dependence, either directly or

indirectly, from claim 1, for the reasons discussed above, and for the additional feature(s) they recite. Thus, claims 1-2, 4-8, and 11-14 are allowable and withdrawal of the rejection of these claims under 35 U.S.C. §103 is respectfully requested.

ii. CLAIM 16 IS PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest a method in a computer system for maintaining and digitally signing a unique, authoritative electronic record, comprising "providing for the receipt of an original electronic record in a repository; providing for the generation of at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record, and wherein the first receipt information is prevented from being transmitted outside the repository; providing for the prepending of the first receipt information at a beginning portion of the original electronic record; providing for the generation of at least some first identifying information, wherein the first identifying information includes a provable representation of the first receipt information; providing for the appending of the first identifying information at an end portion of the original electronic record; providing for the storage of the original electronic record with the prepended first receipt information and the appended first identifying information in the repository as a unique, authoritative electronic record; providing for the receipt of a request to review and optionally sign the authoritative electronic record at a remote location; providing for the computation of a partially completed message digest of the authoritative electronic record, wherein the partially completed message digest is related to a proper subset of the authoritative electronic record; providing for the computation of a complement of the proper subset of the authoritative electronic record; providing for the transmission of the partially completed message digest of the authoritative electronic record to the remote location; providing for the transmission of the complement of the proper subset of the authoritative electronic record to the remote location; providing for the completion of the computation of the message digest of the authoritative electronic record, at the remote location, using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; providing for the display of the complement of the proper subset of the authoritative electronic record at the remote location; providing for the allowance of the generation of at least some digital signature information at the remote location, wherein the digital signature information is generated using a private key and the message digest of the authoritative electronic record;

providing for the receipt of the digital signature information in the repository; providing for the determination of whether the digital signature information represents a valid digital signature; providing for the amendment, if the digital signature information is determined to represent a valid digital signature, of the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information; providing for the generation of at least some additional receipt information, wherein the additional receipt information includes information relating to the signed authoritative electronic record; providing for the prepending of the additional receipt information at a beginning portion of the signed authoritative electronic record; providing for the generation of at least some additional identifying information, wherein the additional identifying information includes a provable representation of the additional receipt information; providing for the appending of the additional identifying information at an end portion of the signed authoritative electronic record; providing for the storing of the signed authoritative electronic record, the additional receipt information, and the additional identifying information, in the repository as the authoritative electronic record, wherein the signed authoritative electronic record includes the digital signature information" (emphasis added), as recited in amended claim 16.

In contrast, as discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document. Additionally, Bisbee discloses forwarding the actual electronic document for review and execution and then, upon receipt of the executed electronic document, authenticating the received electronic document with the appended electronic signature.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest providing for the computation of a partial message digest of a proper subset of the authoritative electronic record; providing for the transmission of the partial message digest and providing for the computation of a message digest, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record. Thus, Bisbee fails to teach the claimed subject matter of original claim 16.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from the method for maintaining and digitally signing a unique, authoritative electronic record, as recited in amended claim 16, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a method in a computer system for maintaining and digitally signing a unique, authoritative electronic record, comprising "providing for the receipt of an original electronic record in a repository; providing for the generation of at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record, and wherein the first receipt information is prevented from being

transmitted outside the repository; providing for the prepending of the first receipt information at a beginning portion of the original electronic record; providing for the generation of at least some first identifying information, wherein the first identifying information includes a provable representation of the first receipt information; providing for the appending of the first identifying information at an end portion of the original electronic record; providing for the storage of the original electronic record with the prepended first receipt information and the appended first identifying information in the repository as a unique, authoritative electronic record; providing for the receipt of a request to review and optionally sign the authoritative electronic record at a remote location; providing for the computation of a partially completed message digest of the authoritative electronic record, wherein the partially completed message digest is related to a proper subset of the authoritative electronic record; providing for the computation of a complement of the proper subset of the authoritative electronic record; providing for the transmission of the partially completed message digest of the authoritative electronic record to the remote location; providing for the transmission of the complement of the proper subset of the authoritative electronic record to the remote location; providing for the completion of the computation of the message digest of the authoritative electronic record, at the remote location, using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; providing for the display of the complement of the proper subset of the authoritative electronic record at the remote location; providing for the allowance of the generation of at least some digital signature information at the remote location, wherein the digital signature information is generated using a private key and the message digest of the authoritative electronic record; providing for the receipt of the digital signature information in the repository; providing for the determination of whether the digital signature information represents a valid digital signature; providing for the amendment, if the digital signature information is determined to represent a valid digital signature, of the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information; providing for the generation of at least some additional receipt information, wherein the additional receipt information includes information relating to the signed authoritative electronic record; providing for the prepending of the additional receipt information at a beginning portion of the signed authoritative electronic record; providing for the generation of at least some additional

identifying information, wherein the additional identifying information includes a provable representation of the additional receipt information; providing for the appending of the additional identifying information at an end portion of the signed authoritative electronic record; providing for the storing of the signed authoritative electronic record, the additional receipt information, and the additional identifying information, in the repository as the authoritative electronic record, wherein the signed authoritative electronic record includes the digital signature information" (emphasis added), as recited in amended claim 16.

Therefore, Applicant respectfully submits that independent claim 16 is patentable over Bisbee in view of Vanstone. Thus, claim 16 is allowable and withdrawal of the rejection of this claim under 35 U.S.C. §103 is respectfully requested.

iii. CLAIMS 22, 23, 24, and 28 ARE PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest a method for displaying, at a remote location, a provable representation of a unique, authoritative electronic record stored in a repository, without compromising the uniqueness of the authoritative electronic record, comprising "receiving a request to review and optionally sign at a remote location a unique, authoritative electronic record stored in a repository, wherein the authoritative electronic record includes at least some first receipt information, which has been prepended at a beginning portion of the authoritative electronic record, and at least some first identifying information, which has been appended at an end portion of the authoritative electronic record, wherein the first receipt information is prevented from being transmitted outside the repository, and wherein the first identifying information includes a provable representation of the first receipt information; computing at the repository a complement of a proper subset of the authoritative electronic record, wherein the complement of the proper subset of the authoritative electronic record is a provable representation of the authoritative electronic record; transmitting the complement of the proper subset of the authoritative electronic record to the remote location; and allowing the complement of the proper subset of the authoritative electronic record to be displayed at the remote location" (emphasis added), as recited in amended claim 22.

In contrast, as discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the

original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing

the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document. Additionally, Bisbee discloses forwarding the actual electronic document for review and execution and then, upon receipt of the executed electronic document, authenticating the received electronic document with the appended electronic signature.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest computing a partial message digest of a proper subset of the authoritative electronic record; transmitting the partial message digest of the authoritative electronic record to the remote location and transmitting the complement of the proper subset of the authoritative electronic record to the remote location.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a method for displaying, at a remote location, a provable representation of a unique, authoritative electronic record stored in a repository, without compromising the uniqueness of the authoritative electronic record, comprising "receiving a request to review and optionally sign at a remote location a unique, authoritative electronic record stored in a repository, wherein the authoritative electronic record includes at least some first receipt information, which has been prepended at a beginning portion of the authoritative electronic record, and at least some first identifying information, which has been appended at an end portion of the authoritative electronic record, wherein the first receipt information is prevented from being transmitted outside the repository, and wherein the first identifying information includes a provable representation of the first receipt information; computing at the repository a complement of a proper subset of the authoritative electronic record, wherein the complement of the proper subset of the authoritative electronic record is a provable representation of the authoritative electronic record; transmitting the complement of the proper subset of the authoritative electronic record to the remote location; and allowing the complement of the proper subset of the authoritative electronic record to be displayed at the remote location" (emphasis added), as recited in amended claim 22, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a method for displaying, at a remote location, a provable representation of a unique, authoritative electronic record stored in a repository, without compromising the uniqueness of the authoritative electronic record, comprising "receiving a request to review and optionally sign at a remote location a unique, authoritative electronic record stored in a repository, wherein the authoritative electronic record includes at least some first receipt information, which has been prepended at a beginning portion of the authoritative electronic record, and at least some first identifying information, which has been appended at an end portion of the authoritative electronic record, wherein the first receipt information is prevented from being transmitted outside the repository, and wherein the first identifying information includes a provable representation of the first receipt information; computing at the repository a complement of a proper subset of the authoritative electronic

record, wherein the complement of the proper subset of the authoritative electronic record is a provable representation of the authoritative electronic record; transmitting the complement of the proper subset of the authoritative electronic record to the remote location; and allowing the complement of the proper subset of the authoritative electronic record to be displayed at the remote location" (emphasis added), as recited in amended claim 22.

Therefore, Applicant respectfully submits that independent claim 22 is patentable over Bisbee in view of Vanstone. Likewise, dependent claims 23, 24, and 28 are also patentable over Bisbee in view of Vanstone by virtue of their dependence, either directly or indirectly, from claim 22, for the reasons discussed above, and for the additional feature(s) they recite. Thus, claims 22, 23, 24, and 28 are allowable and withdrawal of the rejection of these claims under 35 U.S.C. §103 is respectfully requested.

iv. CLAIM 30 IS PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest a method for generating a digital signature at a remote location for a unique, authoritative electronic record which resides in a repository, without compromising the uniqueness of the authoritative electronic record, comprising "computing at the repository a complement of a proper subset of the authoritative electronic record; transmitting to the remote location the complement of the proper subset of the authoritative electronic record; computing at the repository a partially completed message digest of the authoritative electronic record, wherein the partially completed message digest is related to the proper subset of the authoritative electronic record; transmitting to the remote location the partially completed message digest of the authoritative electronic record; allowing the computation of the message digest of the authoritative electronic record to be completed at the remote location using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; and allowing the generation of at least some digital signature information at the remote location, wherein the digital signature information is generated using a private key and the message digest of the authoritative electronic record" (emphasis added), as recited in amended claim 30.

In contrast, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an

executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and

appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Thus, Bisbee discloses forwarding the actual electronic document for review and execution and then, upon receipt of the executed electronic document, authenticating the received electronic document with the appended electronic signature.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest receiving a complement of the proper subset of the authoritative electronic record from a repository; receiving a partial message digest of the authoritative electronic record from a repository.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a method for generating a digital signature at a remote location for a unique, authoritative electronic record which resides in a repository, without compromising the uniqueness of the authoritative electronic record, comprising "computing at the repository a complement of a proper subset of the authoritative electronic record; transmitting to the remote location the complement of the proper subset of the authoritative electronic record; computing at the repository a partially completed message

digest of the authoritative electronic record, wherein the partially completed message digest is related to the proper subset of the authoritative electronic record; transmitting to the remote location the partially completed message digest of the authoritative electronic record; allowing the computation of the message digest of the authoritative electronic record to be completed at the remote location using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; and allowing the generation of at least some digital signature information at the remote location, wherein the digital signature information is generated using a private key and the message digest of the authoritative electronic record" (emphasis added), as recited in amended claim 30, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a method for generating a digital signature at a remote location for a unique, authoritative electronic record which resides in a repository, without compromising the uniqueness of the authoritative electronic record, comprising "computing at the repository a complement of a proper subset of the authoritative electronic record; transmitting to the remote location the complement of the proper subset of the authoritative electronic record; computing at the repository a partially completed message digest of the authoritative electronic record, wherein the partially completed message digest is related to the proper subset of the authoritative electronic record; transmitting to the remote location the partially completed message digest of the authoritative electronic record; allowing the computation of the message digest of the authoritative electronic record to be completed at the remote location using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; and allowing the generation of at least some digital signature information at the remote location, wherein the digital signature information is generated using a private key and the message digest of the authoritative electronic record" (emphasis added), as recited in amended claim 30.

Therefore, Applicant respectfully submits that independent claim 30 is patentable over Bisbee in view of Vanstone. Thus, claim 30 is allowable and withdrawal of the rejection of this claim under 35 U.S.C. §103 is respectfully requested.

v. CLAIMS 31-34 ARE PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest a method for including a valid digital signature, computed at a remote location, in a unique, authoritative electronic record stored in a repository, without compromising the uniqueness of the authoritative electronic record, wherein the authoritative electronic record includes at least some first receipt information which has been prepended at a beginning portion of the authoritative electronic record, and at least some first identifying information which has been appended at an end portion of the authoritative electronic record, wherein the first receipt information is prevented from being transmitted outside the repository, and wherein the first identifying information includes a provable representation of the first receipt information, comprising "receiving in the repository at least some digital signature information, wherein the digital signature information was generated at a remote location using a private key and a message digest, wherein the message digest was computed using a partially completed message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record, wherein the partially completed message digest is related to the proper subset of the authoritative electronic record; determining whether the digital signature information represents a valid digital signature; amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information; and storing the signed authoritative electronic record in the repository as the authoritative electronic record." (emphasis added), as recited in amended claim 31.

In contrast, as discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally

signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the

document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest that the message digest is computed using a partial message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record. Thus, Bisbee fails to teach the claimed subject matter of original claim 31.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a method for including a valid digital signature, computed at a remote location, in a unique, authoritative electronic record stored in a repository, without compromising the uniqueness of the authoritative electronic record, wherein the authoritative electronic record includes at least some first receipt information which has been prepended at a beginning portion of the authoritative electronic record, and at least some first identifying information which has been appended at an end portion of the authoritative electronic record, wherein the first receipt information is prevented from being transmitted outside the repository, and wherein the first identifying information includes a provable representation of the first receipt information, comprising "receiving in the repository at least some digital signature information, wherein the digital

signature information was generated at a remote location using a private key and a message digest, wherein the message digest was computed using a partially completed message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record, wherein the partially completed message digest is related to the proper subset of the authoritative electronic record; determining whether the digital signature information represents a valid digital signature; amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information; and storing the signed authoritative electronic record in the repository as the authoritative electronic record." (emphasis added), as recited in amended claim 31, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a method for including a valid digital signature, computed at a remote location, in a unique, authoritative electronic record stored in a repository, without compromising the uniqueness of the authoritative electronic record, wherein the authoritative electronic record includes at least some first receipt information which has been prepended at a beginning portion of the authoritative electronic record, and at least some first identifying information which has been appended at an end portion of the authoritative electronic record, wherein the first receipt information is prevented from being transmitted outside the repository, and wherein the first identifying information includes a provable representation of the first receipt information, comprising "receiving in the repository at least some digital signature information, wherein the digital signature information was generated at a remote location using a private key and a message digest, wherein the message digest was computed using a partially completed message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record, wherein the partially completed message digest is related to the proper subset of the authoritative electronic record; determining whether the digital signature information represents a valid digital signature; amending, if the digital signature information is determined to represent a valid digital

signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information; and storing the signed authoritative electronic record in the repository as the authoritative electronic record." (emphasis added), as recited in amended claim 31.

Therefore, Applicant respectfully submits that independent claim 31 is patentable over Bisbee in view of Vanstone. Likewise, dependent claims 32-34 are also patentable over Bisbee in view of Vanstone by virtue of their dependence, either directly or indirectly, from claim 31, for the reasons discussed above, and for the additional feature(s) they recite. Thus, claims 31-34 are allowable and withdrawal of the rejection of these claims under 35 U.S.C. §103 is respectfully requested.

vi. CLAIM 36 IS PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest a computer system for maintaining and updating a unique, authoritative electronic record, comprising "means for receiving an original electronic record in a repository; means for generating at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record, and wherein the first receipt information is prevented from being transmitted outside the repository; means for prepending the first receipt information at a beginning portion of the original electronic record; means for generating at least some first identifying information, wherein the first identifying information includes a provable representation of the first receipt information; means for appending the first identifying information at an end portion of the original electronic record; means for storing the original electronic record with the prepended first receipt information and the appended first identifying information in the repository as a unique, authoritative electronic record; means for receiving a request to review and optionally sign the authoritative electronic record at a remote location; means for computing a partially completed message digest of the authoritative electronic record, wherein the partially completed message digest is related to a proper subset of the authoritative electronic record; means for computing a complement of the proper subset of the authoritative electronic record; means for transmitting to the remote location the partially completed message digest of the authoritative electronic record; means for transmitting to the remote location the complement of the proper subset of the authoritative electronic record; means for completing the computation of the message digest

of the authoritative electronic record, at the remote location, using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; means for displaying the complement of the proper subset of the authoritative electronic record at the remote location; means for allowing the generation of at least some digital signature information at the remote location, wherein the digital signature information is generated using a private key and the message digest of the authoritative electronic record; means for receiving the digital signature information in the repository; means for determining whether the digital signature information represents a valid digital signature; means for amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information; means for generating at least some additional receipt information, wherein the additional receipt information includes information relating to the signed authoritative electronic record; means for prepending the additional receipt information at a beginning portion of the signed authoritative electronic record; means for generating at least some additional identifying information, wherein the additional identifying information includes a provable representation of the additional receipt information; means for appending the additional identifying information at an end portion of the signed authoritative electronic record; and means for storing the signed authoritative electronic record, the additional receipt information, and the additional identifying information, in the repository as the authoritative electronic record, wherein the signed authoritative electronic record includes the digital signature information" (emphasis added), as recited in amended claim 36.

In contrast, as discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically

(including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by

itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document. Additionally, Bisbee discloses forwarding the actual electronic document for review and execution and then, upon receipt of the executed electronic document, authenticating the received electronic document with the appended electronic signature.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest means for computing a partial message digest of a proper subset of the authoritative electronic record; means for transmitting the partial message digest and means for computing a message digest, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record. Thus, Bisbee fails to teach the claimed subject matter of original claim 36.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a computer system for maintaining and updating a unique, authoritative electronic record, as recited in amended claim 36, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a computer system for maintaining and updating a unique, authoritative electronic record, comprising "means for receiving an original electronic record in a repository; means for generating at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record, and wherein the first receipt information is prevented from being transmitted outside the repository; means for prepending the first receipt information at a beginning portion of the original electronic record; means for generating at least some first identifying information, wherein the first identifying information includes a provable representation of the first receipt information; means for appending the first identifying information at an end portion of the original electronic record; means for storing the original electronic record with the prepended first receipt information and the appended first identifying information in the repository as a unique, authoritative electronic record; means for receiving a request to review and optionally sign the authoritative electronic record at a remote location; means for computing a partially completed message digest of the authoritative electronic record, wherein the partially completed message digest is related to a proper subset of the authoritative electronic record; means for computing a complement of the proper subset of the authoritative electronic record; means for transmitting to the remote location the partially completed message digest of the authoritative electronic record; means for transmitting to the remote location the complement of the proper subset of the authoritative electronic record; means for completing the computation of the message digest of the authoritative electronic record, at the remote location, using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; means for displaying the complement of the proper subset of the authoritative electronic record at the remote location; means for allowing the generation of at least some digital signature information at the remote location, wherein the digital signature information is generated using a private key and the message digest of the authoritative electronic record; means for receiving the digital signature information in the repository; means for determining whether the digital signature information represents a valid digital signature; means for amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the

digital signature information; means for generating at least some additional receipt information, wherein the additional receipt information includes information relating to the signed authoritative electronic record; means for prepending the additional receipt information at a beginning portion of the signed authoritative electronic record; means for generating at least some additional identifying information, wherein the additional identifying information includes a provable representation of the additional receipt information; means for appending the additional identifying information at an end portion of the signed authoritative electronic record; and means for storing the signed authoritative electronic record, the additional receipt information, and the additional identifying information, in the repository as the authoritative electronic record, wherein the signed authoritative electronic record includes the digital signature information" (emphasis added), as recited in amended claim 36.

Therefore, Applicant respectfully submits that independent claim 36 is patentable over Bisbee in view of Vanstone. Thus, claim 36 is allowable and withdrawal of the rejection of this claim under 35 U.S.C. §103 is respectfully requested.

vii. CLAIM 38 IS PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest a system for obtaining a digital signature from a remote location for a unique, authoritative electronic record, which resides in a repository, without compromising the uniqueness of the authoritative electronic record, the system comprising "a software program that is capable of receiving a request to review, and optionally sign, at a remote location a unique, authoritative electronic record stored in a repository, wherein the authoritative electronic record includes at least some first receipt information which has been prepended at a beginning portion of the authoritative electronic record, and at least some first identifying information which has been appended at an end portion of the authoritative electronic record, wherein the first receipt information is prevented from being transmitted outside the repository, and wherein the first identifying information includes a provable representation of the first receipt information; a software program that is capable of computing at the repository a complement of a proper subset of the authoritative electronic record; a software program that is capable of computing at the repository a partially completed message digest of the authoritative electronic record, wherein the partially completed message digest is related to the proper subset of the authoritative electronic record; a software program that is capable of controlling the transmission of the

complement of the proper subset of the authoritative electronic record and the partially completed message digest of the authoritative electronic record to the remote location; a software program that is capable of allowing the computation of the message digest of the authoritative electronic record to be completed at the remote location using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; a software program that is capable of allowing the complement of the proper subset of the authoritative electronic record to be displayed at the remote location; and a software program that is capable of allowing the generation of at least some digital signature information at the remote location, wherein the digital signature information is generated using a private key and the message digest of the authoritative electronic record" (emphasis added), as recited in amended claim 38.

In contrast, as discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic

disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document. Additionally, Bisbee discloses forwarding the actual electronic document for review and execution and then, upon receipt of the executed electronic document, authenticating the received electronic document with the appended electronic signature.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest a software program that is capable of computing a partial message digest of a proper subset of the authoritative electronic record; a software program that is capable of controlling the transmission of the complement of the proper subset of the authoritative electronic record, the partial message digest and the complement of the proper subset of the authoritative electronic record to the remote location; a software program that is capable of allowing a message

digest to be computed, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a system for obtaining a digital signature from a remote location for a unique, authoritative electronic record, which resides in a repository, without compromising the uniqueness of the authoritative electronic record, as recited in amended claim 38, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a system for obtaining a digital signature from a remote location for a unique, authoritative electronic record, which resides in a repository, without compromising the uniqueness of the authoritative electronic record, the system comprising "a software program that is capable of receiving a request to review, and optionally sign, at a remote location a unique, authoritative electronic record stored in a repository, wherein the authoritative electronic record includes at least some first receipt information which has been prepended at a beginning portion of the authoritative electronic record, and at least some first identifying information which has been appended at an end portion of the authoritative

electronic record, wherein the first receipt information is prevented from being transmitted outside the repository, and wherein the first identifying information includes a provable representation of the first receipt information; a software program that is capable of computing at the repository a complement of a proper subset of the authoritative electronic record; a software program that is capable of computing at the repository a partially completed message digest of the authoritative electronic record, wherein the partially completed message digest is related to the proper subset of the authoritative electronic record; a software program that is capable of controlling the transmission of the complement of the proper subset of the authoritative electronic record and the partially completed message digest of the authoritative electronic record to the remote location; a software program that is capable of allowing the computation of the message digest of the authoritative electronic record to be completed at the remote location using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; a software program that is capable of allowing the complement of the proper subset of the authoritative electronic record to be displayed at the remote location; and a software program that is capable of allowing the generation of at least some digital signature information at the remote location, wherein the digital signature information is generated using a private key and the message digest of the authoritative electronic record" (emphasis added), as recited in amended claim 38.

Therefore, Applicant respectfully submits that independent claim 38 is patentable over Bisbee in view of Vanstone. Thus, claim 38 is allowable and withdrawal of the rejection of this claim under 35 U.S.C. §103 is respectfully requested.

viii. CLAIM 39 IS PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest a system for including a valid digital signature, computed at a remote location, in a unique, authoritative electronic record stored in a repository, without compromising the uniqueness of the authoritative electronic record, wherein the authoritative electronic record includes at least some first receipt information which has been prepended at a beginning portion of the authoritative electronic record, and at least some first identifying information which has been appended at an end portion of the authoritative electronic record, wherein the first receipt information is prevented from being transmitted outside the repository, and wherein the first identifying information includes a provable representation of the first receipt information, comprising "a software program that

is capable of receiving in the repository at least some digital signature information, wherein the digital signature information was generated at a remote location using a private key and a message digest, wherein the message digest was computed using a partially completed message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record, wherein the partially completed message digest is related to the proper subset of the authoritative electronic record; a software program that is capable of determining whether the digital signature information represents a valid digital signature; a software program that is capable of amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information; and a software program that is capable of storing the signed authoritative electronic record in the repository as the authoritative electronic record" (emphasis added), as recited in amended claim 39.

In contrast, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way

that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document. Additionally, Bisbee discloses forwarding the actual electronic document for review and execution and then, upon receipt of the executed electronic document, authenticating the received electronic document with the appended electronic signature.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest that the computed message digest is generated using a partial message digest of the authoritative electronic record and a Complement of a proper subset of the authoritative electronic record.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a system for including a valid digital signature, computed at a remote location, in a unique, authoritative electronic record stored in a repository, without compromising the uniqueness of the authoritative electronic record, as recited in amended claim 39, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a system for including a valid digital signature, computed at a remote location, in a unique, authoritative electronic record stored in a repository, without compromising the uniqueness of the authoritative electronic record, wherein the authoritative electronic record includes at least some first receipt information which has been prepended at a beginning portion of the authoritative electronic record, and at least some first identifying information which has been appended at an end portion of the authoritative electronic record, wherein the first receipt information is prevented from being transmitted outside the repository, and wherein the first identifying information includes a provable representation of the first receipt information, comprising "a software program that is capable of receiving in the repository at least some digital signature information, wherein the digital signature

information was generated at a remote location using a private key and a message digest, wherein the message digest was computed using a partially completed message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record, wherein the partially completed message digest is related to the proper subset of the authoritative electronic record; a software program that is capable of determining whether the digital signature information represents a valid digital signature; a software program that is capable of amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information; and a software program that is capable of storing the signed authoritative electronic record in the repository as the authoritative electronic record" (emphasis added), as recited in amended claim 39.

Therefore, Applicant respectfully submits that independent claim 39 is patentable over Bisbee in view of Vanstone. Thus, claim 39 is allowable and withdrawal of the rejection of this claim under 35 U.S.C. §103 is respectfully requested.

ix. CLAIM 40 IS PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest a computer program product for obtaining a digital signature on a single authoritative copy of an original electronic record, comprising "a computer usable medium and computer readable code embodied on the computer usable medium for obtaining a digital signature on a single authoritative copy of an original electronic record, the computer readable code comprising: computer readable program code devices configured to cause the computer to effect the storing of an original electronic record as an authoritative electronic record in a repository; computer readable program code devices configured to cause the computer to effect the transmission of a complement of a proper subset of the authoritative electronic record and a partially completed message digest of the authoritative electronic record, wherein the complement of the proper subset of the authoritative electronic record is a provable representation of the authoritative electronic record, and wherein the partially completed message digest of the authoritative electronic record is related to the proper subset of the authoritative electronic record; computer readable program code devices configured to cause the computer to effect the allowance of the generation of at least some digital signature information, wherein the digital

signature information is produced using a computed message digest and a private key, wherein the computed message digest is generated using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; computer readable program code devices configured to cause the computer to effect the transmission of the digital signature information from the remote location to the repository and the receipt of the digital signature information in the repository; computer readable program code devices configured to cause the computer to effect the amending, if the received digital signature information is determined to be valid, of the authoritative electronic record in the repository to include at least some of the received digital signature information" (emphasis added), as recited in amended claim 40.

In contrast, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to

obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Thus, Bisbee discloses forwarding the actual electronic document for review and execution and then, upon receipt of the executed electronic document, authenticating the received electronic document with the appended electronic signature.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest a computer readable program code device configured to cause the computer to effect the transmission of a provable representation of an authoritative electronic record from a repository to a remote location, wherein the provable representation of the authoritative electronic record includes a partial message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record and the computed message digest is generated using the partial message digest of the authoritative electronic record and the complement of a proper subset of the authoritative electronic record.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption

key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a computer program product for obtaining a digital signature on a single authoritative copy of an original electronic record, as recited in amended claim 40, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a computer program product for obtaining a digital signature on a single authoritative copy of an original electronic record, comprising "a computer usable medium and computer readable code embodied on the computer usable medium for obtaining a digital signature on a single authoritative copy of an original electronic record, the computer readable code comprising: computer readable program code devices configured to cause the computer to effect the storing of an original electronic record as an authoritative electronic record in a repository; computer readable program code devices configured to cause the computer to effect the transmission of a complement of a proper subset of the authoritative electronic record and a partially completed message digest of the authoritative electronic record, wherein the complement of the proper subset of the authoritative electronic record is a provable representation of the authoritative electronic record, and wherein the partially completed message digest of the authoritative electronic record is related to the proper subset of the authoritative electronic record; computer readable program code devices configured to cause the computer to effect the allowance of the generation of at least some digital signature information, wherein the digital signature information is produced using a

computed message digest and a private key, wherein the computed message digest is generated using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; computer readable program code devices configured to cause the computer to effect the transmission of the digital signature information from the remote location to the repository and the receipt of the digital signature information in the repository; computer readable program code devices configured to cause the computer to effect the amending, if the received digital signature information is determined to be valid, of the authoritative electronic record in the repository to include at least some of the received digital signature information" (emphasis added), as recited in amended claim 40.

Therefore, Applicant respectfully submits that independent claim 40 is patentable over Bisbee in view of Vanstone. Thus, claim 40 is allowable and withdrawal of the rejection of these claims under 35 U.S.C. §103 is respectfully requested.

III. NEW CLAIMS 41-50 ARE PATENTABLE

A. NEW CLAIMS 41-45 ARE PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For the reasons discussed above, Applicant respectfully submits that independent claim 30 is patentable over Bisbee in view of Vanstone. Likewise, new dependent claims 41-45 are also patentable over Bisbee in view of Vanstone by virtue of their dependence, either directly or indirectly, from claim 30, for the reasons discussed above, and for the additional feature(s) they recite.

B. NEW CLAIMS 46-50 ARE PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For the reasons discussed above, Applicant respectfully submits that independent claim 33 is patentable over Bisbee in view of Vanstone. Likewise, new dependent claims 46-50 are also patentable over Bisbee in view of Vanstone by virtue of their dependence, either directly or indirectly, from claim 33, for the reasons discussed above, and for the additional feature(s) they recite.

CONCLUSION

Based on the foregoing amendments and remarks, Applicant respectfully submits that claims 1, 2, 4-8, 11-14, 16-18, 20-24, 28, 30-34, and 36-50 are directed to allowable subject matter and that the application is in condition for allowance. Accordingly, prompt reconsideration and allowance of the application with these claims is respectfully requested.

However, if the Examiner believes there is anything further necessary to place this application in better condition for allowance, Applicant requests the Examiner telephone Applicant's undersigned representative at the number listed below.

Respectfully submitted,

Peter A. Shaddock II
Registration No. 44,331

Date: April 3, 2006

Bowman Green Hampton & Kelly, PLLC
501 Independence Parkway, Suite 201
Chesapeake, VA 23320-5173

Telephone: (757) 548-2323
Fax: (757) 548-2345
E-mail: pshaddock@bghklaw.net